

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

GOOGLE LLC,

Plaintiff,

v.

Civil Action No. 1:21-cv-10260-DLC

DMITRY STAROVIKOV;
ALEXANDER FILIPPOV;
Does 1-15,

Defendants.

**FINAL DEFAULT JUDGMENT AND ORDER
FOR PERMANENT INJUNCTION**

This matter came before the Court on Plaintiff's Google LLC ("Google") Motion for Default Judgment and Entry of Permanent Injunction. The Court finds that Google has established the elements of its claims under: the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. §§ 1962(c)–(d); the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2701; the Lanham Act, 15 U.S.C. §§ 1114, 1125; tortious interference with business relations; and unjust enrichment.

Defendants John Does 1–15 ("Doe Defendants") have been properly served but failed to answer, plead, or otherwise defend this Action, and the prerequisites for a permanent injunction have all been met. Google is therefore entitled to default judgment under Rule 55(b) and a permanent injunction pursuant to Rule 65 of the

Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a), and 28 U.S.C. § 1651(a) (the All-Writs Act).

THE COURT HEREBY FINDS THAT:

Jurisdiction and Venue

1. This Court has federal-question jurisdiction over Google’s claims under the Racketeer Influenced and Corrupt Organizations Act, the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the Lanham Act under 28 U.S.C. § 1331. This Court also has jurisdiction over the Lanham Act and related state and common law unfair competition claims under 28 U.S.C. § 1338 and 15 U.S.C. § 1121, respectively. This court has supplemental jurisdiction over the state-law claims under 28 U.S.C. § 1367.

2. This Court has personal jurisdiction over the Doe Defendants because:

- a. Doe Defendants distribute malware to Google users in this district and within the state of New York;
- b. Doe Defendants send commands to infected user computers in this district and within New York to carry out illicit schemes;
- c. Google’s Complaint and supporting papers demonstrate that the Doe Defendants undertook these activities intentionally with knowledge that their actions would cause harm to users in New York, and cause Google harm in New York; and
- d. Google does business in New York and has done business in New York for many years.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Doe Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. §

1391(6) and 18 U.S.C. § 1965 because: a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district; a substantial part of the property that is the subject of Google's claims is situated in this judicial district; a substantial part of the harm caused by Doe Defendants has occurred in this judicial district; and Doe Defendants transact their affairs in this judicial district. Moreover, Doe Defendants are subject to personal jurisdiction in this district and no other venue appears to be more appropriate.

Default Judgment

4. Doe Defendants were properly served with the summons, complaint, and the other pleadings in this Action. Doe Defendants received adequate notice of this Action, in satisfaction of due process requirements and as required by Fed. R. Civ. P. 4. Specifically, Doe Defendants have been served by email, text message (including by WhatsApp), and publication on a publicly available website. Doe Defendants also have actual notice of these proceedings based on (a) widespread media coverage of this case, including in Russia, that specifically mentions Google's claims against Defendants Starovikov and Filippov and several of their unnamed associates, (b) Google's disruption of the botnet's activity and Defendants' actions in response thereto, and (c) two prominent co-conspirators' actual notice of, and active participation in, this lawsuit.

5. Doe Defendants have failed to appear, plead, or otherwise defend against this Action. The requisite time of 21 days between service of the summons

and complaint has elapsed. The Clerk properly entered default pursuant to Rule 55(a) on June 10, 2022. ECF No. 85.

6. The evidence indicates that no Doe Defendant is an infant or incompetent.

7. The factual allegations in the complaint, which are deemed admitted by Doe Defendants' default, and the further evidence in Google's supporting papers establish that Doe Defendants are liable for violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1962(c)–(d) (Count I); the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (Count II), the Electronic Communications Privacy Act, 18 U.S.C. § 2701 (Count III), Lanham Act, 15 U.S.C. §§ 1114, 1125 (Count IV), and for tortious interference with business relations and unjust enrichment (Counts V–VI).

8. *RICO*. The Doe Defendants have violated and continue to violate the RICO statute.

- a. The Doe Defendants were, and still are, active participants in the operation and management of the Glupteba botnet with direct ties to a C2 server previously associated with proxying activity on infected machines.
- b. Google has established that the Doe Defendants formed an enterprise. The Doe Defendants shared a common purpose to spread malware to build a botnet that is deployed for numerous criminal schemes for profit.
- c. Google has established that the Doe Defendants engaged in a pattern of racketeering activity. The predicate acts include three separate violations of the CFAA. The Doe Defendants have violated and continue to violate the CFAA, resulting in damage as defined in § 1030(c)(4)(A)(i)(VI), by (1) infecting protected computers with malware, (2) transmitting to such

protected computers programs designed to carry out their schemes, and (3) transmitting to such protected computers commands to infected computers. Google has shown that the Doe Defendants committed other predicate acts, including violations of the federal wire fraud statute, 18 U.S.C. § 1343, federal identity fraud statute, 18 U.S.C. § 1028, and federal access device fraud statute, 18 U.S.C. § 1029.

- d. Google has suffered injury to its business or property as a result of Doe Defendants' acts that constitute these predicate offenses.

9. *CFAA*. The Doe Defendants have violated and continue to violate the Computer Fraud and Abuse Act. The CFAA prohibits, among other things, intentionally accessing a protected computer, without authorization, and thereby obtaining information from that computer. *See* 18 U.S.C. § 1030(a)(2)(C). The Doe Defendants intentionally accessed thousands of users' computers operating in interstate commerce through the internet, without authorization, to infect them with malware. They did so to obtain information such as account credentials and URL history, which they have then sold to others. This has affected well over ten computers within a one-year span and resulted in damages in excess of \$5,000.

10. *ECPA*. The Doe Defendants have violated and continue to violate the Electronic Communications Privacy Act. The ECPA prohibits, among other things, "intentionally access[ing] without authorization a facility through which an electronic communication service is provided" to "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701(a). The Doe Defendants have deliberately broken into the accounts of Google users and thereby obtained unauthorized access to emails and other communications stored on Google servers.

11. *Lanham Act.* The Doe Defendants violated the Lanham Act by using Google’s YouTube mark—a valid, protectable, registered and incontestable trademark—in commerce in a manner likely to have caused confusion among consumers by operating a website that used the YouTube mark in the domain name and on the landing page. *See* 15 U.S.C. § 1114(1). In addition, the Lanham Act makes unlawful a false or misleading representation, including a false designation of origin, that “in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of . . . goods, services, or commercial activities.” 15 U.S.C. § 1125(a)(1)(B). The Doe Defendants deceived internet users by falsely marketing their malware as software for downloading videos from YouTube, for their own profit, to the detriment of Google and Google’s trademarks. By establishing the Doe Defendants’ liability under the Lanham Act, Google is also entitled to a presumption of irreparable harm. 15 U.S.C. § 1116(a).

12. Google has shown that the Doe Defendants are liable for New York common law claims of tortious interference with business relationships and unjust enrichment.

A Permanent Injunction is Warranted

13. “It is well-established that a court may grant a permanent injunction as part of a default judgment.” *Ideavillage Prod. Corp. v. OhMyGod 1*, 2020 WL 6747033, at *4 (S.D.N.Y. Nov. 17, 2020). “Whether to issue a permanent injunction in such a case depends on (1) the likelihood that plaintiff will suffer irreparable harm if an injunction is not granted; (2) whether remedies at law such as monetary

damages are inadequate to compensate plaintiff for that harm; (3) the balance of hardships; and (4) whether the public interest would not be disserved by a permanent injunction.” *Id.* (citing *Salinger v. Colting*, 607 F.3d 68, 77–78 (2d Cir. 2010)). The Court finds that Google has established each of these factors and that a permanent injunction is warranted.

14. *Irreparable Harm and Inadequate Remedies at Law.* Google has established that it was irreparably injured and that legal remedies are inadequate to compensate for that harm. In particular, it has shown that the Doe Defendants—through their participation in, and operation of, the Glupteba Enterprise—have threatened the security of the internet, including Google platforms, by transmitting malware through the internet to configure, deploy, and operate a botnet. The Enterprise has distributed malware on devices of Google users, compromising the security of those devices and continues to issue commands to those devices to carry out criminal activities, such as selling access to Google user accounts and selling fraudulent credit cards to use on those accounts.

15. The Doe Defendants control a botnet that has infected more than one million devices. At any moment, the botnet’s extraordinary computing power could be harnessed as part of additional criminal schemes. Doe Defendants could, for example, enable large ransomware or distributed denial-of-service attacks on legitimate businesses and other targets. Doe Defendants could themselves perpetrate such a harmful attack, or they could sell access to the botnet to a third-party for that purpose.

16. In addition, the Doe Defendants' conduct continues to infringe Google's trademarks, injure Google's goodwill, and damage its reputation by creating confusion as to the source of the Glupteba malware. This constitutes irreparable harm.

17. *Balance of the Hardships.* The equities also favor a permanent injunction. The criminal enterprise defrauded, and continues to defraud, consumers and injures Google. There is no countervailing factor weighing against a permanent injunction as there is no legitimate reason why Doe Defendants should be permitted to continue to disseminate malware and manipulate infected computers to carry out criminal schemes.

18. *Public Interest.* Google has shown that the public interest favors granting a permanent injunction. Every day that passes, there is substantial risk that Doe Defendants may infect new computers, steal more account information, and deceive more unsuspecting victims. After receiving notice of the Temporary Restraining Order and Preliminary Injunction, Doe Defendants have continued to engage in conduct enjoined by this Court's Orders. Doe Defendants have attempted to establish new C2 servers in response to Google's ongoing disruption efforts and have continued to establish new websites in order to reconstitute Glupteba Enterprise storefronts and provide Glupteba Enterprise customers continued access to their accounts. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest, and the public interest is clearly served by enforcing

statutes designed to protect the public, such as RICO, the CFAA, the ECPA, and the Lanham Act.

FINAL JUDGMENT AND PERMANENT INJUNCTION

IT IS HEREBY ORDERED that Google's Motion for Default Judgment and Entry of a Permanent Injunction is granted.

IT IS FURTHER ORDERED that Doe Defendants are in default, and that judgment is awarded in favor of Google and against Doe Defendants.

IT IS FURTHER ORDERED that Doe Defendants, any of their officers, agents, servants, employees, attorneys, and all others in active concert or participation with them, who receive actual notice of this Order by personal service or otherwise including via email ("Restrained Parties"), are permanently restrained and enjoined from, anywhere in the world:

1. Intentionally accessing and sending malicious code to Google or the protected computers of Google's customers without authorization;
2. Sending malicious code to configure, deploy, and/or operate a botnet;
3. Attacking and compromising the security of the computers or networks of Google's users;
4. Stealing and exfiltrating information from computers or computer networks;

5. Creating websites that falsely indicate that such websites are or were associated with Google, YouTube, or any other Google affiliate, including through use of Google's YouTube mark or other false or misleading representations;

6. Configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in Google's pleadings, including but not limited to the C2 servers hosted at, and operating through, the IP Addresses listed in Appendix A to Google's Complaint and through any other component or element of the botnet in any location;

7. Delivering malicious code designed to steal credentials and cookies;

8. Monitoring the activities of Google or Google's customers;

9. Stealing information from Google or Google's customers;

10. Selling access to the accounts of Google's customers;

11. Corrupting applications on victims' computers and networks, thereby using such computers or networks to carry out the foregoing activities;

12. Offering or promoting credit cards to others for use in purchasing services from Google;

13. Misappropriating that which rightfully belongs to Google, Google's customers and users, or that in which Google has a proprietary interest;

14. Using, linking to, transferring, selling, exercising control over, or otherwise owning or accessing domains connected with the Enterprise, its activities, or its use of the botnet;

15. Using, transferring, exercising control over, or accessing any accounts used in the transfer of money or electronic currency, including cryptocurrency, or in the processing of card-based transactions, as a means to further Doe Defendants' unlawful schemes;

16. Using and infringing Google's trademarks, including Google's YouTube mark;

17. Using, in connection with Doe Defendants' activities, any products or services with any false or deceptive designation, representations or descriptions of Doe Defendants or of their activities, whether by symbols, words, designs, or statements, which would damage or injure Google or its customers or users or give Doe Defendants an unfair competitive advantage or result in deception of consumers;

18. Acting in any other manner which suggests in any way that Doe Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Google, or otherwise passing off Doe Defendants' activities, products or services as Google's; and

19. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

Upon service by email, text message, or internet publication, the Doe Defendants and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of the Default Judgment and Permanent Injunction Order, and any act by any of the Doe Defendants or the Restrained Parties in violation of any of

the terms of the Default Judgment and Permanent Injunction Order may be considered and prosecuted as contempt of Court.

IT IS FURTHER ORDERED that Google may serve this Order on the persons and entities providing services, including domain name registrars, name servers, web hosting services, and other internet service providers, relating to the domains and IP addresses identified by Google as connected to the Enterprise, its activities, or its botnet, requesting that those persons and entities take reasonable best efforts to implement the following actions:

1. Take reasonable steps to identify incoming and/or outgoing internet traffic on their respective networks that originates and/or is being sent from and/or to such identified domains and IP addresses;

2. Take reasonable steps to block incoming and/or outgoing internet traffic on their respective networks that originate and/or are being sent from and/or to such identified domains and IP addresses except as explicitly provided for in this Order;

3. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Doe Defendants or Doe Defendants' representatives moved the botnet infrastructure, to ensure that Doe Defendants cannot use such infrastructure to control the botnet;

4. Disable completely the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with such identified domains and IP addresses and make them inaccessible from any other

computer on the internet, any internal network, or in any other manner, to Doe Defendants, Doe Defendants' representatives, and all other persons, except as otherwise ordered herein;

5. Completely, and until further order of this Court, suspend all services to Doe Defendants or Doe Defendants' representatives or resellers associated with such identified domains and IP addresses;

6. Refrain from providing any notice or warning to, or communicating in any way with Doe Defendants or Doe Defendants' representatives until the steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

7. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Doe Defendants or Doe Defendants' representatives associated with such identified domains and IP addresses, including, without limitation, not enabling, facilitating, and/or allowing Doe Defendants or Doe Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other domains and IP addresses;

8. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Doe Defendants and Doe Defendants' representatives operating or controlling such identified domains and IP addresses, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access

and contact records and all records, documents and logs associated with the use of or access to such domains and IP addresses;

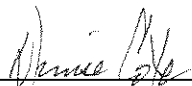
9. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

10. Completely preserve the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with such identified domains and IP addresses, and preserve all evidence of any kind related to the content, data, software, or accounts associated with such domains, IP addresses, and computer hardware.

IT IS FURTHER ORDERED that Google may serve this Order upon such persons as Google determines are necessary to address and enjoin activity associated with domains and IP addresses identified by Google as being used in connection with the Enterprise, its activities and its botnet, without seeking further leave of the court.

So ordered.

Sept. 30, 2022



DENISE COTE
United States District Judge